A CONCEPT OF OPERATIONS FOR USING SENSORS IN COLLECTIVE PROTECTION

Steven S. Streetman
ENSCO, Inc.
5400 Port Royal Rd.
Springfield, VA 22151-2312
703-321-4463

ABSTRACT

This paper describes concepts of operation for using sensors to monitor passive collective protection strategies and initiate active collective protection strategies. To effectively use sensors, in many cases true sensor integration must be performed where information from multiple sensors (to include chemical or biological agent sensors, meteorological information, and internal air flow information) is automatically analyzed as a single Event and responses are determined from the collective sensor evidence. This paper describes the trade-offs and current philosophy behind which measures are initiated based on sensor inputs and which require operator validation or external approval for initiation. Examples from operational experience will illustrate these trade-offs. From these examples, guidelines for passive vs. active collective protection for real life scenarios may be inferred.

INTRODUCTION

Collective protection methodologies may be classified into two types: passive, strategies that are continuously providing collective protection, and active, strategies that are implemented during an event. Sensors may play a role in both types of collective protection methodologies, but are often critical for active strategies since they require a trigger to initiate. In this paper we discuss the role of sensors in collective protection. Certainly, sensors that detect chemical, biological, radiological, or nuclear (CBRN) agents play a significant role in collective protection strategies, but other sensor types such meteorological, pressure or flow, equipment status, CCTV, acoustic, and fire can often be vital to appropriate implementation of collective protection methodologies.

SENSOR ROLES IN PASSIVE STRATEGIES

Since sensors are not required for initiation of passive strategies, their role is less critical during a CBRN event. Instead, sensors are required on a continuing basis to ensure proper operation of the strategies. Sensors monitor passive strategies to provide feedback on their status, identify maintenance activities, and measure their effectiveness. In one operational system, a passive, continuously operational positive pressure environment was maintained for a critical area. Differential pressure sensors were used to ensure that there was sufficient pressure between the area and the outside air and between the area and adjacent areas not served by the positive pressure system. In addition, differential pressure sensors were monitored to determine flow loss across multiple filter banks within the positive pressure system itself to alert operators to unusual changes in the pressure that would indicate filter failure or clogging.

Another common passive strategy involves sealing the building against leaks and incorporating airlocks to reduce the introduction of contaminant from an external release. If the passive strategy relies on eliminating leaks, simple balanced magnetic switches on doors and windows can ensure the strategies are effective by alerting operators to open windows or doors that are propped open.

It is interesting to note that the sensors of most utility in supporting passive strategies tend to be pressure, flow, and security sensors that are well-known, inexpensive, easy to use, and extremely reliable COTS products rather than CBRN detectors. Typically sensors may be used independently of each other; no sensor integration or fusion is required to support passive strategies, though integration of multiple sensors may assist in an overall evaluation of the collective strategy.

USING CBRN SENSORS AS TRIGGERS

The remainder of this paper will focus on using sensors in active collective protection strategies. We begin by discussing the challenges faced when using CBRN sensors and identify techniques that can, to a great extent, overcome these challenges. We will continue with a discussion of how to characterize and verify sensor alarms, an important step in using sensors operationally, and complete the discussion by describing how sensors are used in the various stages of an event to actuate active collective protection strategies.

CBRN sensors give false alarms. CBRN sensors give nuisance alarms. For the foreseeable future, it will be the case that using these sensors will require verification and analysis before any catastrophic measures may be taken in response to a sensor detection. Methodologies have been identified and implemented for automated processing of the alarms. Additional manual and analysis methodologies have been identified and codified in procedures for operational systems. This combination of automated procedures and manual analysis can be used to overcome the limitations of existing CBRN sensors.

The essential problem is one of information. CBRN sensors provide detections. What that generally means (the actual information content of the detection) is that some internal threshold was exceeded on a system that measures a quantity related to chemicals, biological particles, or gamma rays. The inference from the detection (the information actually sent to an operator) is generally an agent identification, to some level of specificity, and an estimate of concentration. On the other hand, what an operator of the collective protection system wants to know is the nature of the event:

- Is there a threat agent?
- Where is the agent (where did it start, where is it now)?
- What is the agent and how much of it?
- Where is it going and how soon will it get there?

It is important to distinguish between what the sensor provides (evidence at some level of confidence that there is an event) from what the operator needs: knowledge that there is an event and information about its nature. There are additional steps required to boost the confidence that there is an event from the sensor's confidence to near certainty. There are steps as well to define where the agent is and where it is going. In short, appropriate use of CBRN sensors requires post-processing to transform the sensors' detection data into actionable information. Common steps are outlined in the following subsections. This paper will focus entirely on CBRN-specific techniques. For a discussion of a general methodology for integrating sensors and developing actionable information, please see (1).

1 *False Alarms vs. Nuisance Alarms*

False and nuisance alarms have been mentioned above. We distinguish between them because the techniques for eliminating them are different. False alarms are alarms without the presence of a threat source (e.g. a sensor identifies sarin when there is no sarin present). False alarms may result from noise on a sensor or from the presence of interferents, sources that the sensor may confuse with threat sources. Virtually all sensors have a non-zero false alarm rate, but false alarm rates may be extremely low. Nuisance alarms, in contrast, are alarms where a correct source is present, but the source is not a threat. Examples include cleaning compounds carried past a sensor. The sensor correctly identifies concentrations of, say, ammonia, but it isn't a large scale ammonia release, just a bucket of cleaning fluid near the sensor. If sensors with low false alarm rates are used, the vast majority of actual alarms are nuisance alarms and interferents.

Reducing false alarms (and nuisance alarms) is a vital process for appropriate use of sensors in collective protection. After the second time an operator evacuates a facility because of a false sensor report, the system will be ignored. There are any number of techniques for reducing false alarms. A few of the most common in the CBRN world are described below.

2 Multi-Sensor Techniques

Multi-sensor techniques either use multiple examples of a single sensor or use multiple types of sensors to assess sensor alarms. Rather complex sensor interactions may be used and have been used in operational facilities but a full treatment of those techniques is beyond the scope of this paper. For purposes of this paper, we will describe five examples of multi-sensor techniques for reducing false/nuisance alarms that are in operational use and give the flavor of additional techniques.

The first technique is essentially to require that more than one sensor detect the same agent. This technique is especially effective against false alarms since sensors with low false alarm rates are extremely unlikely to detect the same agent at the same time in the absence of any actual cause. For nuisance alarms, this technique is less effective since there is a cause for the alarm that would likely set off both sensors. However, many nuisance sources are so localized and many sensor deployments are so sparse, that requiring two sensors to detect can eliminate nuisance alarms as well as false alarms. The risk is of missing an alarm that is only detectable at a single sensor location. For this reason, there is often a rating of the seriousness of an alarm and while single detections are always analyzed for verification, multiple alarms immediately result in an increased response level.

A similar technique to the multiple sensor detects is that of using orthogonal sensors. In theory, sensors that depend on different phenomenologies for detection may be likely to react differently to interferent sources (sources that can cause false alarms). The technique is to co-locate two different phenomenologies for identifying, say, a chemical agent. If only one of the sensors detects, it is likely to correspond to an interferent that does not trigger the other sensor. A true threat source would trigger both sensors to detect. As with the first technique, this technique does not eliminate nuisance alarms since the nuisance alarms involve substances both sensors are designed to detect. This technique is generally successful, however, against false alarms, including alarms from interferents.

A third technique involves integrating two sensor types that detect the same things but provide different types of information or have different strengths. An example from the radiologic community is to use fairly simple gamma detectors to identify radiation sources because they work quickly and then to use more time consuming isotope identification sensors as back-ups to determine whether the radiation detected is a threat. Using the simple sensors allows rapid processing (required for most applications). The additional time required by the isotope identification sensors is then focused only on known radiation sources.

Another validation system primarily for chemical sensors is to provide CCTV camera coverage of the area near the sensors. An operator can then determine visually whether people in the vicinity of the detection are in distress. Seeing video of the area provides visual confirmation of a chemical event and may allow determination of source location or release methodology.

Finally, a typical response to a sensor detection is to send trained personnel to the site. Personnel will often bring handheld sensors that independently verify the type of agent. Such sensors are available for chemical, biological, and radiological agents. Additional verification of biological agents is typically done in a laboratory setting with samples taken from the site by response personnel. These additional procedures with back-up sensors are not performed in real time, but are often vital to avoid initiating catastrophic procedures from false alarms.

3 Single Sensor Techniques

In addition to multi-sensor techniques, there are often integration techniques that can be performed with a single sensor's evidence to reduce or eliminate false alarms and nuisance alarms. The techniques fall into two primary categories: integrating over time, and reviewing intermediate data.

Integrating over time relies on the fact that, for a significant release of a threat agent, the agent is likely to remain present in the area around the sensor at detectable (and likely increasing) quantities for multiple processing iterations. An integration system would look at multiple detections over time from a single sensor as more indicative of an actual threat than a single detection. Again, this technique does not remove the responsibility for analyzing and validating all alarms. Rather, it provides indications that certain alarms are higher confidence and more likely to involve real threats. This technique is effective against both false and nuisance alarms since nuisance alarms are often more transitory than real events.

Many of the more modern sensors will provide the intermediate evidence that was used to determine the detection upon request. Such quantities as particle counts and fluorescence results from biological sensors, surface acoustic wave frequency history and ion mobility spectrometer spectra from chemical sensors, and radiation counts and spectra from radiologic and nuclear sensors can provide useful evidence in assessing alarms. Data that show very brief and marginal crossing of the detection threshold are less compelling than data that rise quickly or move well above the detection threshold. In addition, intermediate sensor data can be compared with site-specific known interferents to tailor sensor performance to a site and eliminate the most common nuisance alarms.

CHARACTERIZING ALARMS

Validated detections only provide a small portion of the information a responder needs to appropriately react to a CBRN event. A sensor will usually provide a detection (presence of some threat agent). Many sensors will identify a class of agent or a specific agent, extremely useful information. Top of the line sensors will provide some coarse determination of concentration (low, medium, high). But sensors by themselves cannot determine the extent or severity of an overall event and cannot predict where agent will go. An integration system that can work appropriately with the sensor data, perform higher level characterization, and run predictive models is essential. ENSCO's SENTRY system is such an integration system. For more information about SENTRY, see (2).

4 Source Location

The key to determining the extent of a release is to find the location of the source. If the location of the source is known, forward modeling may be performed and compared to actual sensor results to estimate the amount of agent released. But determining the source location is not possible using only sensor detections from CBRN sensors. There are at least five methods of varying accuracy and utility for determining the source location:

- Eye Witness: a responder finds the source and reports its location (primary current method). This method is accurate, but may be of low utility if the source is not found until after the event is over. This method is more effective as a verification tool for an automated, but less reliable, location capability.
- Camera: the source is seen on camera. This method can be extremely fast if there are automated methods for viewing cameras associated with events or if there are video analysis capabilities such as video motion detection that can steer operators to appropriate cameras quickly. This method has the added advantage over the eye witness method that the responder is not at risk while looking for the source. However, cameras can't see everywhere and some sources may not provide a visual cue.
- Stand-off Detectors: Stand-off detectors for chemical and biological agents can provide a set of bearings and elevations to map the cloud. Multiple stand-off sensors, or a single mobile stand-off sensor can provide a map of the actual agent location for external releases. These detectors are an excellent solution since they provide both actual measured location and

automated detection of the agent itself. However, the technology is only fielded for chemical detection of a limited number of agents and Toxic Industrial Chemicals (TICs) and for biological particles. In addition, the sensors are extremely expensive and, thus, may not be always available to a particular facility or region.

- Acoustic TDOA: For explosive sources, acoustic sensors may provide a location based on the time difference of arrival (TDOA) of the acoustic wave at time synced networks of acoustic sensors. This technique assumes the deployment of acoustic sensors (similar to the gunshot detection networks deployed in several small cities). In demonstrations, accurate locations have been automatically determined from networks of sensors several kilometers apart. This technique only works for explosive sources, however, and difficult environments such as urban canyons may create a multi-path situation that degrades or destroys the capability.
- Modeling: Work is currently in progress for determining estimated source locations based on air flow modeling and sensor detections for interior releases (see (3)). Similar work has been proposed for external releases. These techniques evaluate potential locations against the actual air flow information and actual sensor detections to determine whether the location is a potential site for the source. The accuracy of the source location in this case is extremely dependent on the numbers and locations of sensors (denser sensor networks generally provide smaller potential source locations). One major advantage of this approach is that meteorological sensors are cheap, readily available, and often already installed. Similarly, for internal releases, modern heating, ventilating, and air conditioning (HVAC) systems often have flow or pressure measurements already available at numerous points throughout a facility. These techniques can then be implemented at existing installations that have CBRN sensors.

Knowing the source location from any one of these methodologies provides extremely useful information for responders and for implementing collective protection strategies. Knowing the source location allows for more precise HVAC-based active strategies then knowing only a general affected region.

5 Predictive Modeling

If a source location methodology is implemented, then using a combination of that methodology and the sensor detection information can provide most of the information that a responder needs to determine when, where, and how to implement collective protection procedures. The final question is where is the contaminant going and how quickly? The answer to this question can only be obtained by predictive modeling. At its simplest, one would expect that contaminant would move downwind and gear protective strategies such as evacuation to avoid areas downwind. However, much more accurate modeling techniques exist for both outside modeling of contaminant flow (e.g. VLSTRACK, HPAC) and internal flows (e.g. CONTAM, COMUS). Integrating these models with sensor detection and analysis capabilities (as in the SENTRY system) allows the best available information to be provided for initiation of collective protection strategies.

SENSOR ROLES IN ACTIVE STRATEGIES

The role of sensors varies through the stages of an event. At onset, CBRN sensors play the primary role triggering validation and response procedures. As an event progresses, the roles of HVAC, meteorological, security, and CCTV sensors become more important. Similarly, the types of collective protection actions performed vary with the type of event and stage of validation. The following section describes the types of actions performed during the stages of an event, beginning with initial operator notification, progressing through initial (pre-verification) actions, actions that perform the alarm verification, additional measures implemented once an alarm has been verified, and actions performed after an event.

1 Notification

For our purposes, an event begins when the first CBRN sensor detects and notifies an operator. At this stage, an operator generally expects the notification to be a false or nuisance alarm since those are infinitely more common than a real attack. As the sensor provides additional alarms or other sensors detect, the information provided to the operator becomes refined as the system integrates the data.

2 Pre-Verification Actions

Once notification has been received, initial response plans are initiated. These generally include event characterization such as source location algorithms and predictive models, but may also include active collective protection strategies. Modifying HVAC parameters to respond to an initial detection may be a good alternative since it

- Provides a measure of protection for the facility occupants
- Is unlikely to be noticed (at least for a few minutes) by occupants and, thus, is not likely to generate alarm
- Is easy to recover from if an alarm is determined to be a false or nuisance alarm

Additional actions may include lock-down of specified entry/exit areas and raising the alarm status of the command center responsible for verifying the alarms.

What is typically not done as a pre-verification action is to alert building occupants or even response personnel, or to initiate any catastrophic action such as building evacuation, setting up safe rooms, requiring personnel to don protective gear, or initiating decontamination procedures.

The reason for performing any response at all prior to verification of the alarm is time. A real release of an agent can be expected to spread very quickly through a facility via the HVAC system or outside from the wind. Every second counts in implementing a response; this is why responses, ideally, are automatic. The verification actions, on the other hand can take anywhere from a few seconds to a few hours. Thus, if a response can be implemented automatically based on an initial alert without causing impact to facility operations, it should be automated. Catastrophic responses that cause severe impact to operations must be reserved for verified alarms.

3 Verification Actions

Again, once notification is received procedures are initiated to verify the alarm. Immediate actions include switching and viewing CCTV information from the area of the sensor. Any multi-sensor or single sensor integration algorithms are implemented (which may include querying nearby sensors for intermediate data).

Responders may be sent to the sensor site to perform handheld sensor measurements or take a sample for forwarding to a lab. Additional in-sensor tests are also performed for some sensor types. Essentially, during this stage the algorithms described earlier in this paper as sensor integration and validation capabilities are performed. The output of this stage is the information required by the responders to respond to an alarm.

If an alarm is judged to be a false or nuisance alarm, any pre-verification actions are reset to the pre-alarm state (e.g. HVAC is returned to previous state, alarm level is lowered).

4 Post-Verification Actions

If an alarm is judged to be real, and that judgement is generally based as much on policy as on technical ability to evaluate an alarm, full-up collective protection procedures are initiated. HVAC may be further, or more drastically, modified. Safe rooms may be set up. The facility or portions of the facility may be evacuated. Notifications will be sent to responders, local and regional law enforcement and emergency response entities, and, potentially, the media.

During this time, sensors provide updates and predictive models will be rerun to account for collective protection actions taken. The sensor data may be compared with the predictive models to provide an assessment of the models' accuracy. CCTV will be continuously monitored and updated information should be passed on to responders and coordinating agencies.

Sensor determined locations and trouble areas may be used to guide responders in setting up control sites and determining safe evacuation paths. Rapid response to a correct location may allow mitigation of the event if it is a continuous release rather than a single burst.

5 Post-Event Actions (Decontamination/Forensics)

After an event is over, sensors may be used to guide reconstitution efforts (to do the critical areas first). Sensors may help determine which areas require which decontamination procedures and may verify when decontaminated areas are safe. In addition, the collected sensor evidence during an event may be used after an event to precisely model the contaminant flow for forensic evidence collection. In fact, sensor triggers may allow automated collection of air samples for later forensic analysis.

CONCLUSIONS

Sensors are important both for monitoring the effectiveness of collective protection strategies and for triggering them. However, given the severe nature of CBRN events and the propensity for sensors to false alarm, post-processing and integration of sensor data and a tiered set of collective response procedures is vital to avoid unwarranted, catastrophic action. Appropriate integration both of CBRN sensors and of other supporting sensor types is necessary to reduce false and nuisance alarms and provide operators with the information they need to appropriately respond to events. A system, such as ENSCO's SENTRY system that can automatically perform much of the sensor integration, enhance the information with source location, deconfliction, and predictive modeling, and simplify the operator's task is an important asset in using sensors for collective protection.

REFERENCES

1. S. S. Streetman, C. D. Carleton, R. G. Hamrick, M. M. McGarvey, "Data Integrator for Ground Sensors (DIGS)" [4743-66] in *Unattended Ground Sensor Technologies and Applications IV*, Edward M. Carapezza, Editor, Proceedings of SPIE Vol. 4743, page numbers (313-319).
2. Steven S. Streetman, "An Operational Sensor Integration, Analysis, Predictive Modeling, and Response Component for CBRN Battle Management", submitted to The First Joint Conference on Battle Management for Nuclear, Chemical, Biological and Radiological Defense, November 4-8, 2002.
3. Dr. Jeff Piotrowski and Mrs. Eileen Corelli, "A Source Location and Collective Protection Tool", presented at COLPRO 2002, poster session